PRIVACY IMPACT ASSESSMENT

Corporate Insurance Information Systems

Risk Management Agency

May 2003

PRIVACY IMPACT ASSESSMENT

Corporate Insurance Information Systems

TABLE OF CONTENTS

Page #

1.0 PRIVACY IMPACT ASSESSMENT METHODOLOGY

This Privacy Impact Assessment (PIA) was completed using the United States Department of Agriculture (USDA) guidelines on privacy dated 24 October 2002. Information was collected from interviews with the data owners of the system, system administrators and developers, and from internal and external audits.

1.1 Background

The USDA is responsible for ensuring the privacy, confidentiality, integrity, and availability of customer and employee information. The USDA recognizes that privacy protection is both a personal and fundamental right of its customers and employees. Among the most basic of customers and employees' rights is an expectation that USDA will protect the confidentiality of personal, financial, and employment information. Customers and employees also have the right to expect that USDA will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities.

1.2 Applicable laws, regulations, policies and procedures

The Federal Crop Insurance Act, as amended (7 USC 1501 et seq., Ch 36)

The Federal Crop Insurance Corporation (7 CFR Subtitle B, Section 4)

Privacy Act of 1974, as amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal Agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503)

Computer Security Act of 1987 (Public Law 100-235), which establishes minimum security practices for Federal computer systems

OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems

Freedom of Information Act, as amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

1.3 Systems of Records Notice

A Systems of Records Notice contains the "rules" of which a system must follow if it houses data on individuals. Each individual system must have its own System of Records Notice. These records can be found in the Federal General Register and in the Privacy Act Issuances that are released every two years by the Government Printing Office. The Systems of Records notices that this investments falls under include:

FCIC-2: FCIC Compliance Review Cases
FCIC-6: Insurance Contract Analysis
FCIC-7: Insurance Contract Files
FCIC-8: List of Ineligible Producers

FCIC-10: Policyholder
FCIC-11: Loss Adjuster

2.0 ROLES AND RESPONSIBILITIES

The agency ISSPM is responsible for completing the PIA on all systems under their control. They will work closely with the system owners and developers to correctly identify privacy risks that are generated from the system. When the PIA is completed, the ISSPM will forward the completed PIA to the Department Privacy Policy Analyst for further analysis and a determination of the need of the system. The Privacy Policy Analyst, ISSPM, and system owner will incorporate design requirements into the system to resolve privacy risks.

3.0 ASSESSMENT

Information in this investment contains, but is not limited to: Social Security Numbers, Producer Names, Tax IDs for Insurance Providers, and Financial Information for Insurance Providers. This data is used to populate several databases that determine the cost of crop insurances, help to determine the total loss (indemnity) and profit (premium) on a policy, and also tacks fraud, waste, and abuse. Systems included in this assessment include: Data Acceptance System, Actuarial Filing System, Compliance Tracking System, and the Corporate Reporting System.

3.1 Data in the system

The data in the system comes primarily from the Insurance Providers through a server that is dedicated to receiving their inputs. Data is also gathered second hand from producers from their insurance applications. The producer provides name, address, Social Security Number/Tax ID Number, type of crop grown, farming practice used, and other relevant farming data. The insurance agent verifies this data at the time of submission. The insurance providers reference this data when submitting information on premium/indemnity to RMA.

Collection of this data is also necessary to process accounting information for payment to/from the Insurance Providers. Provisions in the Standard Reinsurance Agreement provide penalties for late submission and erroneous data submission; it is therefore in the best interests of the Insurance Providers to ensure that the data is correct and current. The Data Acceptance System verifies that this data is not a duplicate of previously submitted data, checks to make sure that it is in the correct format as specified by RMA, and that the producer is not on the ineligible producer list. When a change to data is made, the file overwrites the entire data file, ensuring that the data stays married to the changes.

The Compliance Tracking System references this data in the investigations and reports that it generates. This data, when used in the Compliance Tracking System, is exempt from the Freedom of Information Act as amended, as stated in the Systems of Records Notice FCIC-2, under the provisions of the FOIA that exempts investigatory material compiled for law enforcement purposes.

3.2 Access to the data

The RMA ISSPM and the branch SLR are responsible for ensuring that privacy is protected through the proper use of security controls. Privacy is treated the same as the basic security tenant of confidentiality when security controls are evaluated and employed on the system. In this manner, while not explicitly a section on security audits and risk assessments, privacy is included in the overall security plan of the system.

Access to the data is limited to the absolute minimum that is necessary to perform a job function. The data owners determine this access. In the case of the Compliance Tracking System, a specific legal investigation will determine the access. Individuals that need access to the data will fill out a FCIC-586 *User Request Form* that is verified by the user's Security Liaison Representative (SLR) and then forwarded to the RMA Security Office. The form specifies what access to which databases is needed by the user. After RMA Security approves the form, the account is created and the appropriate Database Administrator assigns the approved access levels.

Systems that access the data have to undergo a cursory approval by the Database Administrator of the affected database, the business owner of the database, RMA Security, and the Chief of the System Administrator Branch. Systems that currently access the data are the RMA Financial Management Systems and the RMA Strategic Data Analysis System. Private insurance providers also have access to the data in the system, but in a sanitized manner (i.e., information that is not submitted by them is not accessible to them, unless personal information has been stripped from the data).

Once the data has left the system for use in other processes and systems, it is the responsibility of that system's SLR to ensure the proper use of the data, but the RMA ISSPM will still maintain control over these systems and audit them for compliance. In the case of the Insurance Providers, there is a Company Representative that interfaces with the RMA Security Office to ensure data privacy. Insurance Providers are bound to follow RMA's security and privacy policies by the terms in the Standard Reinsurance Agreement.

3.3 Attributes of the data

The information in this system is necessary for the implementation and maintenance of the Federal Crop Insurance Program. This information allows RMA and the private Insurance Providers to determine actuarial rates (i.e., the rates for crop insurance) and to determine the effectiveness of the Crop Insurance Program. It also allows for the tracking of claims and the system has been developed so that it allows a myriad of different queries based on the attributes of the data. Data that is presented to third parties is sanitized (i.e., all the Social Security Number and names have been removed).

Reports on individuals can be accessed using Social Security Number or Names. These reports can be used to determine rates, coverage, types of insurance, and other reports based on agent, loss adjustor, and/or producer. These reports will be available to RMA employees and Compliance Officials. Reports offered to third parties (including Insurance Providers) will be sanitized.

3.4 Maintenance of Administrative controls

This system does not take into account race, sex, national origin, or other attributes that may be used in a matter that does not meet with the requirements of the Risk Management Agency, United States Department of Agriculture, or the Constitution of the United States of America. As such, it has been designed to report only on attributes such as Social Security Number (for agent and producer) and items such as indemnity, premium owed, and crop insured, as an example.

The retention of data is dependent on the system and the media that is used. Computerized (soft-copy) data is maintained indefinitely, with hard copy data being destroyed consistent with the guidance of the National Archivist for all systems, with the exception of Insurance Contract data, which is destroyed after three years.

This system does have the ability to track and monitor individuals, but not explicitly. Reports have to be manually generated and have a specific legal purpose before they are run. The Agency's Privacy Officer must approve these reports before they can be submitted. Information can be used to develop reports that can be used in the detection of fraud, waste, and abuse. In fact, any report that deals with the business of crop insurance, from producers and agents to crops and loss can be run from this system.

The Compliance Tracking System has been designed to specifically track individuals through case files and is used as the investigative tool for fraud, waste, and abuse. This system is exempt from certain provisions in the Privacy Act and Freedom of Information Act as would effect the activities of law enforcement.

4.0 SUMMARY

Privacy is an ongoing process that is becoming evermore entwined with security in Information Systems. The USDA is committed to protecting customer and employee data by addressing the following issues in regards to privacy:

1. The use of information must be controlled

2. Information may only be used for a necessary and lawful purpose.

3. Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.

4. Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.

5. Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Privacy could be affected if information in this system is compromised. RMA has taken steps to treat this information as critical information to its business functions. As such, this information

has been included into the Security Plans and Risk Assessments that cover the individual systems in this investment.

4.1 Points of Contact

Investment Owner: Denise Hoffman; Director Reinsurance Services Division
(816) 926-3406 denise.hoffman@rma.usda.gov

Investment Manager: Lonnie Clemon; Chief, Fiscal Operations Branch
(816) 926-3038 lonnie.clemon@rma.usda.gov

IT Security Manager: Karen Grissom; Information Systems Security Manager
(816) 926-1341 karen.grissom@rma.usda.gov

IT Security Officer: Eric Baer – CISSP; Information Security Officer
(816) 823-1950 eric.baer@rma.usda.gov